

DOCKET No.

NAI1P024\_01.038.01

U.S. PATENT APPLICATION  
FOR AN  
METHOD AND APPARATUS FOR TRANSFERRING  
DATA FROM AN ATM CONNECTION TABLE TO  
MEMORY FOR USE BY AN APPLICATION  
PROGRAM

ASSIGNEE: NETWORKS ASSOCIATES TECHNOLOGY, INC.

KEVIN J. ZILKA  
PATENT AGENT  
P.O. Box 721120  
SAN JOSE, CA 95172

# METHOD AND APPARATUS FOR TRANSFERRING DATA FROM AN ATM CONNECTION TABLE TO MEMORY FOR USE BY AN APPLICATION PROGRAM

5

## RELATED APPLICATION(S)

The present application claims priority from a provisional patent application filed 08/16/01 under serial number 60/313,039, which is incorporated herein by reference.

10

## FIELD OF THE INVENTION

The present invention relates to network analysis systems, and more particularly to monitoring a network for analysis purposes.

15

## BACKGROUND OF THE INVENTION

With the advent of the Internet, there has been a sharp increase in the demand for network bandwidth which has been principally driven by two trends: (i) the increasing number of networked computers exchanging data; and (ii) the increasing need for networked computers to exchange ever-increasing quantities of data. In response to this demand, a variety of new computer network technologies have been developed that improve upon existing technologies by increasing the efficiency of data transmission, increasing the speed of data transmission, or both. Although such technologies achieve increased network bandwidth, they also create a need for new and improved technologies to analyze networks incorporating these technologies.

Network assessment tools referred to as “analyzers” are often relied upon to analyze networks during use. One example of such analyzers is the SNIFFER ANALYZER™ device manufactured by NETWORK ASSOCIATES, INC™. All analyzers have similar objectives such as determining why network performance is slow, understanding the specifics about excessive traffic, and/or gaining visibility into various parts of the network.

Analizers are often used to monitor networks which are based on an asynchronous transfer mode (ATM) switching protocol. ATM switching is used in communications systems for switching voice, data, and video information. Frequently, these services are supported simultaneously by the same switch. In use, ATM switches are capable of switching small elements of information, called cells, rapidly between an input port and an output port. A header at the beginning of each cell contains identifying information that may also be modified in the course of this switching. During operation, the switches typically track the switching using connection tables, stored in a specialized memory in the switch.

In the prior art, each connection supported by the switch occupies at least one entry in one or more of the connection tables. Typical analyzer tools extract these entries for gathering statistics and monitoring various network parameters. To date, such entries have been extracted one-at-a-time. In other words, typically analyzers issue one call command to extract one entry from the connection table. This one-to-one relation thus results in a vast number of calls being made to extract the necessary data.

Since typical scanning is carried out in real-time, it is often difficult to extract all of the required information in a manner efficient enough to keep up with the operation of the switch. Often, the analyzer must take incomplete “snap shots” of the contents of

the connection tables. This, in turn, results in incomplete statistics and substandard scanning results.

There is thus a need for an apparatus and method for more efficiently and  
5 effectively collecting information from ATM connection tables for analysis purposes.

NAI1P024\_01.038.01

### **DISCLOSURE OF THE INVENTION**

A system, method and computer program product are provided for copying data from an asynchronous transfer mode (ATM) connection table. In use, an ATM connection table on an ATM network is monitored. During such monitoring, it is determined whether entries of the ATM connection table are active. If the entries are active, associated data is periodically transferred from the active entries of the ATM connection table to memory. Identifiers associated with the data are utilized for identification purposes. The transferred data in the memory may then be subsequently utilized with an application program.

In one embodiment, the data may be transferred from the active entries of a plurality of ATM connection tables. Such plurality of ATM connection tables may include one ATM connection table for each of a plurality of ATM links. As an option, the plurality of ATM connection tables may include at least one common ATM connection table.

In another embodiment, the entries of the ATM connection table may be deemed active if the entries have been just created since a previous transfer of data. Further, the entries of the ATM connection table may be deemed active if the entries have been altered since a previous transfer of data. As an option, the data from the active entries of the ATM connection table may include statistical information and/or state information.

In still another embodiment, a period with which the data is periodically transferred from the active entries of the ATM connection table to the memory may be configurable. Moreover, the period may be configurable within a predetermined range.

Optionally, the predetermined range may be between 1 transfer/second to 4 transfers/second.

As an option, the periodic transfer of the data may be initiated utilizing an application program interface between the application program and the memory. The periodic transfer of the data may also be ceased utilizing the application program interface between the application program and the memory. Such application program interface may be capable of identifying a location in the memory to which the data is to be transferred. Further, the application program interface may identify a period at which the data is to be transferred to the memory. Still yet, the data from each entry of the ATM connection table may be transferred independently.

In still yet another embodiment, the memory may be interrupted in order for the application program to use the transferred data. Optionally, multiple instances of the data may be stored in the memory. Moreover, the memory may store the data in a circular manner.

It should be noted that the aforementioned identifiers may include ATM connection identifiers. During use, such identifiers may be translated per the desires of the user. In use, an age of the data may be tracked so that the data may be deleted upon the age reaching a predetermined amount.

**BRIEF DESCRIPTION OF THE DRAWINGS**

5      Figure 1 is a schematic diagram of a network architecture, in accordance with one embodiment.

Figure 2 illustrates the transfer of the entries between the connection table and analyzer memory, in accordance with one embodiment.

10      Figure 3 shows a method for copying data from the connection table such as the ATM connection table shown in Figures 1 and 2.

Figure 4 illustrates a method that is executed in parallel with the method of Figure 3 for clearing the entries that have been transferred to the memory.

15

### **DESCRIPTION OF THE PREFERRED EMBODIMENTS**

5           Figure 1 illustrates an exemplary architecture 100, in accordance with one embodiment. As shown, at least one input device 102 is provided along with at least one output device 104. In the context of the present description, the input device 102 and the output device 104 may be any networked device that is capable of receiving and sending communications, respectively. For example, the input and output devices may  
10   include a desktop computer, lap-top computer, hand-held computer, printer or any other type of logic.

Each input device 102 and output device 104 of the present architecture 100 is coupled by way of a network 106. In the context of the present architecture 100, the  
15   network 106 may take any form including, but not limited to a local area network (LAN), a wide area network (WAN) such as the Internet, etc.

As shown in Figure 1, coupled to the network 106 is an analyzer 108. Such analyzer may be coupled to a gateway, switch, input device 102, output device 104, or  
20   any other networked device or logic. In an embodiment where the analyzer 108 is coupled to an Internet switch, the switch may be an Asynchronous Transfer Mode (ATM) switch, a Frame Relay switch or any other switch that acts on units of user data usually called data cells.

25           As is well known, each cell has an identifying section such as a header, used for routing or identifying purposes. The data cells can represent actual data as from a computer, voice, video, or any other type of information. The present embodiment is

described in terms of an ATM switch. However, the same technology can be applied to other types of switches as well.

As shown, the analyzer **108** includes at least one input port **110** and an output  
5 port **112** coupled to the input device **102** and the output device **104**, respectively. An  
ATM core **114** is coupled between the input port **110** and the output port **112**. In use,  
each input port **110** interfaces and connects to one or more of the input devices **102** for  
passing fully formed ATM cells to the ATM core **114**. The output port **112** accepts  
fully formed cells and emits them to one or more of the output devices **104**. It should be  
10 noted that the ATM core **114** may emit cells to a plurality of output ports represented by  
output port **112**, and may send a plurality of copies of the cell to a single output port  
**112**, each with a different header.

The ATM core **114** includes a certain number of connection slots to be  
15 configured for connecting the input ports represented by input port **110** and the output  
ports represented by the output port **112**, or to be idle. Also included is a connection  
table **116** coupled to the ATM core **114** for tracking each connection supported by the  
ATM core **114** in a plurality of entries.

20 It should be noted that the analyzer **108** may be separate from or integral with  
the aforementioned components. In one embodiment, the analyzer **108** may be a  
standalone device which monitors the traffic/segment between two ATM switches  
[Network to Network Interface (NNI)] or between an ATM end-station and a switch  
[User to Network Interface (UNI)].

25

A computer **118** may be coupled to the analyzer **108** or constitute a component  
of the analyzer **108** for extracting such entries from the connection table **116** for  
gathering statistics and monitoring various network parameters. Such statistics and

network parameters may then be used to troubleshoot, monitor network performance, and/or enhance security provisions, i.e. detect attacks, vulnerabilities, malicious code, etc.

5           Unlike prior art analyzers, the present embodiment extracts the entries from the connection table **116** by copying multiple entries into memory. This allows a more comprehensive collection of statistics with respect to the prior art method of extracting entries one-at-a-time.

10           Figure **2** illustrates the transfer of the entries between the connection table **116** and analyzer memory **202**, in accordance with one embodiment. It should be noted that the analyzer memory **202** may be a component of the computer **118** of Figure **1**, dedicated memory, or any other desired memory located in any desired location. In use, the data stored in the ATM connection table may include statistical information, state  
15           information, protocol information, or any other data capable of being used to enhance the operation and security of the architecture **100**. In one embodiment, the analyzer memory **202** may include at least 4Kbytes.

As shown in Figure **2**, the connection table **116** includes a plurality of active  
20           entries **204** and a plurality of idle entries **206**. In one embodiment, the entries of the connection table **116** may be deemed active if the entries have been just created since a previous transfer of data. Further, the entries of the connection table **116** may be deemed active if the entries have been altered since a previous transfer of data. Still yet, a portion of the connection table **116** may be left unused.

25

It should be noted that a plurality of such connection tables **116** may be provided. In such embodiment, one ATM connection table may be provided for each of

a plurality of ATM links. Further, the plurality of ATM connection tables may include at least one common ATM connection table.

Figure 3 illustrates a method **300** for copying data from a connection table such as the ATM connection table shown in Figures 1 and 2. In operation **302**, the ATM connection table is monitored. Upon a triggering event, the entries in the ATM connection table are copied over into memory. In one embodiment, the triggering event may be a periodic interrupt signal generated by the analyzer. It should be noted, however, that the triggering event may be produced by any desired logic that determines when it is appropriate for the entries in the ATM connection table to be copied over into memory.

In one embodiment, a period with which the interrupt signal is generated may be configurable. Moreover, the period may be configurable within a predetermined range. Optionally, the predetermined range may be between 1 transfer/second to 4 transfers/second. This range may ensure optimal transfer of data to enable a comprehensive statistical analysis by the analyzer.

Once it is determined in decision **304** that the interrupt is received, the various entries of the ATM connection table are identified. Note operation **306**. The purpose of such identification process may be to identify which entries of the ATM connection table are suitable for transfer to the memory. In particular, it is determined in decision **310** whether the identified entries are active. As mentioned earlier, the entries of the connection table may be deemed active if the entries have been just created since a previous transfer of data, the entries have been altered since a previous transfer of data, or the entries are in any other way ready to be transferred.

If the entries are deemed active in decision **310**, data is transferred from such entries of the ATM connection table to memory. See operation **312**. Next, in decision **314**, it is determined whether any additional entries exist. If so, a next entry of the ATM connection table is identified in operation **315**, and operation **312** is repeated for any additional active entries. Optionally, multiple instances of the data of each entry may be stored in the memory, if the resources of the memory are sufficient. While an independent transfer of entries is set forth hereinabove, it should be understood that contiguous entries may be transferred at once if supported by the accompanying hardware.

Moreover, the memory may store the data in a circular manner. In other words, the data may be transferred from the ATM connection table to the entries in the memory in sequential order from a first entry to a last entry in the memory. Once the last entry in the memory is filled, the process may be repeated at the first entry.

As mentioned earlier, the data may be transferred from the active entries of a plurality of ATM connection tables, where each ATM connection table corresponds to one of a plurality of ATM links. Further, the plurality of ATM connection tables may include at least one common ATM connection table from which entries are extracted.

Once it is has been determined in decision **314** that no further additional entries exist, an application program associated with the analyzer may be prompted to use the entries transferred to the memory. See operation **316**. So that the application program may use the entries transferred to the memory, identifiers associated with the data may be utilized for identification purposes. It should be noted that such identifiers may include ATM connection identifiers. As an option, such identifiers may be translated into a "CAM ID" which is traditionally used by the ATM core.

As an option, the periodic transfer of the data may be initiated utilizing an application program interface between the application program and the memory. The periodic transfer of the data may also be ceased utilizing the application program interface. Such application program interface may be further capable of identifying a location in the memory to which the entry data is to be transferred. Further, the application program interface may identify a period at which the data is to be transferred to the memory.

By periodically initiating the transfer of all active entries to memory, a more complete set of data is collected for use by the analyzer when monitoring an associated architecture. Further, by storing the entries in the memory, the application program is given adequate time to adequately analyze the entry data. As an option, the memory transfer method 300 may be interrupted in order to further ensure that the application program has adequate time to use the transferred data.

Figure 4 illustrates a method 400 that is executed in parallel with the method 300 of Figure 3 for clearing the entries that have been transferred to the memory. It should be noted that the method 400 may be continuously executed while the method 300 of Figure 3 is being used to extract entries from the connection table.

As shown, one of the entries is identified in operation 402 after which it is determined in decision 404 whether the age thereof has exceeded a predetermined amount. Such predetermined age may be selected based on when the usefulness of an entry is conventionally depleted. If such age has been exceeded, the entry may be cleared in operation 406.

After the entry is cleared or it is determined in decision 404 that the age of the present entry has not exceeded the predetermined amount, a next entry is identified.

Note operation **408**. By this design, the entries may be sequentially checked to determine whether the age has exceeded the threshold, and deleted accordingly in order to make room for additional incoming transferred data.

- 5           While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

10

Patent Application No. 10/000,000